

Orthogonal involutions and totally singular quadratic forms in characteristic two

A.-H. Nokhodkar

Abstract

We associate to every central simple algebra with involution of orthogonal type in characteristic two a totally singular quadratic form which reflects certain anisotropy properties of the involution. It is shown that this quadratic form can be used to classify totally decomposable algebras with orthogonal involution. Also, using this form, a criterion is obtained for an orthogonal involution on a split algebra to be conjugated to the transpose involution.

Mathematics Subject Classification: 16W10, 16K20, 11E39, 11E04.

1 Introduction

The theory of algebras with involution is closely related to the theory of bilinear forms. Assigning to every symmetric or anti-symmetric regular bilinear form on a finite-dimensional vector space V its adjoint involution induces a one-to-one correspondence between the similarity classes of bilinear forms on V and involutions of the first kind on the endomorphism algebra $\text{End}_F(V)$ (see [5, p. 1]). Under this correspondence several basic properties of involutions reflect analogous properties of bilinear forms. For example a symmetric or anti-symmetric bilinear form is isotropic (resp. anisotropic, hyperbolic) if and only if its adjoint involution is isotropic (resp. anisotropic, hyperbolic).

Let (A, σ) be a totally decomposable algebra with orthogonal involution over a field F of characteristic two. In [3], a bilinear Pfister form $\mathfrak{Pf}(A, \sigma)$ was associated to (A, σ) , which determines the isotropy behaviour of (A, σ) . It was shown that for every splitting field K of A , the involution σ_K on A_K becomes adjoint to the bilinear form $\mathfrak{Pf}(A, \sigma)_K$ (see [3, (7.5)]). Also, according to [7, (6.5)] this invariant can be used to determine the conjugacy class of the involution σ on A .

In this work we associate to every algebra with orthogonal involution (A, σ) in characteristic two a pair $(S(A, \sigma), q_\sigma)$ where $S(A, \sigma)$ is a subalgebra of A and q_σ is a totally singular quadratic form on $S(A, \sigma)$. Using this pair, we find in Theorem 3.7 some criteria for σ to be *direct* (a stronger notion than anisotropy defined in [2]). As a consequence, several sufficient conditions for anisotropy of σ are obtained in Corollary 3.10. Further, it is shown in Theorem 3.14 that q_σ can classify the transpose involution on a split algebra. For the case where (A, σ) is totally decomposable, using the quadratic space $(S(A, \sigma), q_\sigma)$ we will complement some results of [3] and [7] in Theorem 4.1 and state several necessary and sufficient conditions for σ to be anisotropic. Finally, we shall

see in Theorem 4.6 and Theorem 4.10 that the form q_σ can be used to find a classification of totally decomposable algebras with orthogonal involution in characteristic two.

2 Preliminaries

In this paper, F denote a field of characteristic two.

Let V be a vector space of finite dimension over F . A bilinear form $\mathfrak{b} : V \times V \rightarrow F$ is called *isotropic* if $\mathfrak{b}(v, v) = 0$ for some $0 \neq v \in V$. Otherwise, \mathfrak{b} is called *anisotropic*. We say that \mathfrak{b} *represents* $\alpha \in F$ if $\mathfrak{b}(v, v) = \alpha$ for some nonzero vector $v \in V$. The set of all elements represented by \mathfrak{b} is denoted by $D(\mathfrak{b})$. If K/F is a field extension, we denote by \mathfrak{b}_K the *scalar extension* of \mathfrak{b} to K . For $\alpha_1, \dots, \alpha_n \in F$ the diagonal bilinear form $\sum_{i=1}^n \alpha_i x_i y_i$ is denoted by $\langle \alpha_1, \dots, \alpha_n \rangle$. Also, the form $\bigotimes_{i=1}^n \langle 1, \alpha_i \rangle$ is called a *bilinear Pfister form* and is denoted by $\langle\langle \alpha_1, \dots, \alpha_n \rangle\rangle$. If \mathfrak{b} is a bilinear Pfister form over F , there exists a bilinear form \mathfrak{b}' , called the *pure subform* of \mathfrak{b} , such that $\mathfrak{b} \simeq \langle 1 \rangle \perp \mathfrak{b}'$. As observed in [1, p. 16] the pure subform of \mathfrak{b} is uniquely determined, up to isometry. According to [4, (6.5)], the form \mathfrak{b} is anisotropic if and only if $\dim_{F^2} Q(\mathfrak{b}) = 2^n$, where $Q(\mathfrak{b}) = D(\mathfrak{b}) \cup \{0\}$.

A *quadratic form* on V is a map $q : V \rightarrow F$ such that (i) $q(\alpha v) = \alpha^2 q(v)$ for $\alpha \in F$ and $v \in V$; (ii) the map $\mathfrak{b}_q : V \times V \rightarrow F$ given by $\mathfrak{b}(v, w) = q(v + w) - q(v) - q(w)$ is an F -bilinear form. A quadratic form q is called *isotropic* if $q(v) = 0$ for some $0 \neq v \in V$ and *anisotropic* otherwise. For a quadratic space (V, q) over F we use the notation $D(q) = \{q(v) \mid 0 \neq v \in V\}$ and $Q(q) = D(q) \cup \{0\}$. The scalar extension of q to an extension K of F is denoted by q_K . A quadratic form q is called *totally singular* if \mathfrak{b}_q is the zero map. For $\alpha_1, \dots, \alpha_n \in F$ the totally singular quadratic form $\sum_{i=1}^n \alpha_i x_i^2$ is denoted by $\langle \alpha_1, \dots, \alpha_n \rangle_q$.

Let A be a central simple algebra over F and let σ be an *involution* on A , i.e., an anti-automorphism of A of order two. We say that σ is of the *first kind* if it restricts to the identity map on F . For a symmetric bilinear space (V, \mathfrak{b}) over F we denote by $\sigma_{\mathfrak{b}}$ the adjoint involution of $\text{End}_F(V)$ with respect to \mathfrak{b} (see [5, p. 1]). An involution σ of the first kind on A is called *symplectic* if it becomes adjoint to an *alternating* bilinear form over a splitting field of A (i.e., a bilinear form \mathfrak{b} with $D(\mathfrak{b}) = 0$). Otherwise, σ is called *orthogonal*. According to [5, (2.6)], σ is orthogonal if and only if $1 \notin \text{Alt}(A, \sigma)$, where $\text{Alt}(A, \sigma) = \{x - \sigma(x) \mid x \in A\}$. The discriminant of an orthogonal involution σ is denoted by $\text{disc } \sigma$ (see [5, (7.1)]). An involution σ is called *isotropic* if $\sigma(x)x = 0$ for some nonzero element $x \in A$. Otherwise, σ is called *anisotropic*.

We will frequently use the following result. Recall that if u is a unit in a central simple algebra A , the *inner automorphism* of A induced by u is defined as $\text{Int}(u)(x) = uxu^{-1}$ for $x \in A$.

Proposition 2.1. *Let $\alpha_1, \dots, \alpha_n \in F^\times$ and let $u \in M_n(F)$ be the diagonal matrix $\text{diag}(\alpha_1, \dots, \alpha_n)$. Consider the involution $\sigma = \text{Int}(u) \circ t$ on $M_n(F)$, where t is the transpose involution. If (V, \mathfrak{b}) is the diagonal bilinear space $\langle \alpha_1, \dots, \alpha_n \rangle$, then $(M_n(F), \sigma) \simeq (\text{End}_F(V), \sigma_{\mathfrak{b}})$.*

Proof. See [5, pp. 13-14]. □

3 The alternator form

For a central simple algebra with orthogonal involution (A, σ) over F we use the following notation:

$$S(A, \sigma) = \{x \in A \mid \sigma(x)x \in F \oplus \text{Alt}(A, \sigma)\}.$$

In other words, $x \in S(A, \sigma)$ if and only if there exists a unique element $\alpha \in F$ such that $\sigma(x)x + \alpha \in \text{Alt}(A, \sigma)$. We denote the element α by $q_\sigma(x)$. Hence, $q_\sigma : S(A, \sigma) \rightarrow F$ is a map satisfying

$$\sigma(x)x + q_\sigma(x) \in \text{Alt}(A, \sigma) \quad \text{for } x \in S(A, \sigma).$$

Lemma 3.1. *Let (A, σ) be a central simple algebra with involution over F . If $x \in \text{Alt}(A, \sigma)$, then $\sigma(y)xy \in \text{Alt}(A, \sigma)$ for every $y \in A$.*

Proof. Write $x = z - \sigma(z)$ for some $z \in A$. Then

$$\sigma(y)xy = \sigma(y)(z - \sigma(z))y = \sigma(y)zy - \sigma(\sigma(y)zy) \in \text{Alt}(A, \sigma). \quad \square$$

Lemma 3.2. *Let (A, σ) be a central simple algebra with orthogonal involution over F . Then*

(i) *$S(A, \sigma)$ is a (unitary) F -subalgebra of A .*

(ii) *$q_\sigma(\lambda x + y) = \lambda^2 q_\sigma(x) + q_\sigma(y)$ and $q_\sigma(xy) = q_\sigma(x)q_\sigma(y)$ for every $\lambda \in F$ and $x, y \in S(A, \sigma)$.*

Proof. For every $\lambda \in F$ we have $\sigma(\lambda)\lambda + \lambda^2 = 0 \in \text{Alt}(A, \sigma)$, so $F \subseteq S(A, \sigma)$. Let $x, y \in S(A, \sigma)$ and $\lambda \in F$. Set $\alpha = q_\sigma(x) \in F$ and $\beta = q_\sigma(y) \in F$. Then

$$\sigma(\lambda x + y)(\lambda x + y) + \lambda^2 \alpha + \beta = \lambda^2(\sigma(x)x + \alpha) + (\sigma(y)y + \beta) + \sigma(\lambda x)y - \sigma(\sigma(\lambda x)y).$$

Hence, $\sigma(\lambda x + y)(\lambda x + y) + \lambda^2 \alpha + \beta \in \text{Alt}(A, \sigma)$, which implies that $\lambda x + y \in S(A, \sigma)$ and $q_\sigma(\lambda x + y) = \lambda^2 \alpha + \beta = \lambda^2 q_\sigma(x) + q_\sigma(y)$. Similarly, using Lemma 3.1 we have

$$\begin{aligned} \sigma(xy)(xy) + \alpha\beta &= \sigma(y)\sigma(x)xy + \alpha\beta = \sigma(y)(\sigma(x)x + \alpha)y + \alpha\sigma(y)y + \alpha\beta \\ &= \sigma(y)(\sigma(x)x + \alpha)y + \alpha(\sigma(y)y + \beta) \in \text{Alt}(A, \sigma). \end{aligned}$$

Hence, $xy \in S(A, \sigma)$ and $q_\sigma(xy) = \alpha\beta = q_\sigma(x)q_\sigma(y)$, proving the result. \square

Corollary 3.3. *Let (A, σ) be a central simple algebra with orthogonal involution over F . Then q_σ is a totally singular quadratic form on $S(A, \sigma)$.*

Proof. The result follows from Lemma 3.2 (ii). \square

Definition 3.4. Let (A, σ) be a central simple algebras with orthogonal involution over F . We call $S(A, \sigma)$ the *alternator subalgebra* of (A, σ) . We also call the quadratic form q_σ the *alternator form* of (A, σ) .

Lemma 3.5. *Let (A, σ) and (A', σ') be two central simple algebras with orthogonal involution over F . If $f : (A, \sigma) \xrightarrow{\sim} (A', \sigma')$ is an isomorphism of algebras with involution, the restriction of f to $S(A, \sigma)$ defines an isometry $(S(A, \sigma), q_\sigma) \xrightarrow{\sim} (S(A', \sigma'), q_{\sigma'})$.*

Proof. For every $x \in S(A, \sigma)$ we have $\sigma(x)x + q_\sigma(x) \in \text{Alt}(A, \sigma)$, which implies that $f(\sigma(x)x + q_\sigma(x)) \in \text{Alt}(A', \sigma')$. Hence, $\sigma'(f(x))f(x) + q_\sigma(x) \in \text{Alt}(A', \sigma')$, i.e., $f(x) \in S(A', \sigma')$ and $q_{\sigma'}(f(x)) = q_\sigma(x)$. \square

The following definition was given in [2].

Definition 3.6. An involution σ on a central simple algebra A is called *direct* if for every $x \in A$ the condition $\sigma(x)x \in \text{Alt}(A, \sigma)$ implies that $x = 0$.

Theorem 3.7. For an orthogonal involution σ on a central simple F -algebra A the following conditions are equivalent:

- (1) σ is direct.
- (2) q_σ is anisotropic.
- (3) $S(A, \sigma)$ is a field.

Moreover, if these conditions hold, then $x^2 \in F$ for all $x \in S(A, \sigma)$.

Proof. The implication (1) \Rightarrow (2) is evident.

(2) \Rightarrow (3) : Since $S(A, \sigma)$ is a subalgebra of A , it suffices to show that (i) $S(A, \sigma)$ contains no zero divisor; (ii) $x^{-1} \in S(A, \sigma)$ for every nonzero element $x \in S(A, \sigma)$; and (iii) $S(A, \sigma)$ is commutative.

Suppose that $xy = 0$ for some $0 \neq x \in S(A, \sigma)$ and $y \in A$. Set $\alpha = q_\sigma(x)$, so that $\sigma(x)x + \alpha \in \text{Alt}(A, \sigma)$. By Lemma 3.1 we have

$$\alpha\sigma(y)y = 0 + \alpha\sigma(y)y = \sigma(y)\sigma(x)xy + \alpha\sigma(y)y = \sigma(y)(\sigma(x)x + \alpha)y \in \text{Alt}(A, \sigma).$$

Since q_σ is anisotropic we have $\alpha \neq 0$. Hence, $y \in S(A, \sigma)$ and $q_\sigma(y) = 0$. Again, the anisotropy of q_σ implies that $y = 0$, proving (i).

To prove (ii) let $0 \neq x \in S(A, \sigma)$ and $\alpha = q_\sigma(x) \neq 0$, so that $\sigma(x)x + \alpha \in \text{Alt}(A, \sigma)$. By Lemma 3.1 we have $\sigma(x^{-1})(\sigma(x)x + \alpha)x^{-1} \in \text{Alt}(A, \sigma)$, i.e., $\alpha\sigma(x^{-1})(x^{-1}) + 1 \in \text{Alt}(A, \sigma)$. It follows that $\sigma(x^{-1})(x^{-1}) + \alpha^{-1} \in \text{Alt}(A, \sigma)$, so $x^{-1} \in S(A, \sigma)$.

Finally, if $x, y \in S(A, \sigma)$, then Lemma 3.2 implies that

$$q_\sigma(xy + yx) = q_\sigma(xy) + q_\sigma(yx) = q_\sigma(x)q_\sigma(y) + q_\sigma(y)q_\sigma(x) = 0.$$

Since q_σ is anisotropic we get $xy = yx$, proving (iii).

(3) \Rightarrow (1) : Suppose that $\sigma(x)x \in \text{Alt}(A, \sigma)$ for some $x \in A$. Then $x \in S(A, \sigma)$ and $q_\sigma(x) = 0$. If $x \neq 0$ then x is a unit, because $S(A, \sigma)$ is a field. Since $\sigma(x)x \in \text{Alt}(A, \sigma)$, Lemma 3.1 implies that $1 = \sigma(x^{-1})\sigma(x)xx^{-1} \in \text{Alt}(A, \sigma)$. This contradicts the orthogonality of σ .

To prove the last statement of the result, let $x \in S(A, \sigma)$ and set $\alpha = q_\sigma(x)$. By 3.2 we have $q_\sigma(x^2) = \alpha^2 = q_\sigma(\alpha)$, so $q_\sigma(x^2 + \alpha) = 0$. As q_σ is anisotropic, we get $x^2 = \alpha \in F$. \square

Lemma 3.8. ([5, (2.26)]) Let (A, σ) be a central simple algebra with orthogonal involution over F . Then the set $\text{Sym}(A, \sigma)$ generates A as an (associative) F -algebra.

Proof. If $\deg_F A > 2$, the result follows from [5, (2.26)]. Suppose that $\deg_F A = 2$. Let $B \subseteq A$ be the subalgebra of A generated by $\text{Sym}(A, \sigma)$. Using the idea of the proof of [5, (2.26)], it is enough to show that $B_K = A_K$ for some extension K of F . Choose an extension K/F with $(A, \sigma)_K \simeq (M_2(K), t)$. The conclusion now easily follows by identifying $\text{Sym}(A, \sigma)_K$ with the set of matrices of the form $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$, where $a, b, c \in K$. \square

Proposition 3.9. *Let (A, σ) be a central simple algebra with orthogonal involution over F . If $S(A, \sigma) \subseteq \text{Sym}(A, \sigma)$, then σ is direct.*

Proof. Suppose that $\sigma(x)x \in \text{Alt}(A, \sigma)$ for some $x \in A$. Then $x \in S(A, \sigma)$, which implies that $\sigma(x) = x$. We claim that $\text{Sym}(A, \sigma) \subseteq C_A(x)$, where $C_A(x)$ is the centralizer of x in A . Let $y \in \text{Sym}(A, \sigma)$. By Lemma 3.1 we have

$$\sigma(xy)xy = \sigma(y)\sigma(x)xy \in \text{Alt}(A, \sigma),$$

hence $xy \in S(A, \sigma) \subseteq \text{Sym}(A, \sigma)$. It follows that $yx = \sigma(y)\sigma(x) = \sigma(xy) = xy$, because the elements x , y and xy are all symmetric. This proves the claim. By Lemma 3.8, $\text{Sym}(A, \sigma)$ generates A as an F -algebra. Hence, $C_A(x) = A$, i.e., $x \in F$. Since σ is orthogonal, the condition $\sigma(x)x \in \text{Alt}(A, \sigma)$ implies that $x = 0$, so σ is direct. \square

Since every direct involution is anisotropic, one can use Theorem 3.7 and Proposition 3.9 to find some sufficient conditions for anisotropy of orthogonal involutions:

Corollary 3.10. *Let (A, σ) be a central simple algebra with orthogonal involution over F . If any of these conditions is satisfied, then σ is anisotropic: (i) q_σ is anisotropic. (ii) $S(A, \sigma)$ is a field. (iii) $S(A, \sigma) \subseteq \text{Sym}(A, \sigma)$.*

Lemma 3.11. *Let (V, \mathfrak{b}) be a symmetric non-alternating bilinear space over F .*

(i) *If $x \in \text{End}_F(V)$, then $\mathfrak{b}(x(v), x(v)) = q_{\sigma_{\mathfrak{b}}}(x)\mathfrak{b}(v, v)$ for every $v \in V$.*

(ii) *If \mathfrak{b} represents 1, then $D(q_{\sigma_{\mathfrak{b}}}) \subseteq D(\mathfrak{b})$.*

Proof. Let $\alpha = q_{\sigma_{\mathfrak{b}}}(x)$, so that $\sigma_{\mathfrak{b}}(x)x + \alpha \in \text{Alt}(\text{End}_F(V), \sigma_{\mathfrak{b}})$. Write $\sigma_{\mathfrak{b}}(x)x = y - \sigma_{\mathfrak{b}}(y) - \alpha$ for some $y \in \text{End}_F(V)$. For every $v \in V$ we have

$$\begin{aligned} \mathfrak{b}(x(v), x(v)) &= \mathfrak{b}((\sigma_{\mathfrak{b}}(x)x)(v), v) = \mathfrak{b}((y - \sigma_{\mathfrak{b}}(y) - \alpha)(v), v) \\ &= \mathfrak{b}(y(v), v) - \mathfrak{b}(\sigma_{\mathfrak{b}}(y)(v), v) - \alpha\mathfrak{b}(v, v) \\ &= \mathfrak{b}(y(v), v) - \mathfrak{b}(v, y(v)) - \alpha\mathfrak{b}(v, v) = \alpha\mathfrak{b}(v, v). \end{aligned}$$

This proves the first part. The second part follows by applying (i) to a vector $v \in V$ with $\mathfrak{b}(v, v) = 1$. \square

Remark 3.12. The converse of Proposition 3.9 does not hold in general. To construct a counter-example, let $\langle\langle \alpha, \beta \rangle\rangle$ be an anisotropic bilinear Pfister form over F and let u be the diagonal matrix $\text{diag}(1, \alpha, \beta, \alpha\beta + 1)$. Consider the involution $\sigma = \text{Int}(u) \circ t$ on $M_4(F)$. By Proposition 2.1 we have $(M_4(F), \sigma) \simeq (\text{End}_F(V), \sigma_{\mathfrak{b}})$, where (V, \mathfrak{b}) is the diagonal bilinear space $\langle 1, \alpha, \beta, \alpha\beta + 1 \rangle$. Since

\mathfrak{b} is anisotropic, the form q_σ is also anisotropic by Lemma 3.11 (ii). Hence, σ is direct by Theorem 3.7. Let

$$x = \begin{pmatrix} 0 & (\alpha\beta)^{-1} & \beta^{-1} & 0 \\ 0 & 0 & 0 & \alpha(1+\alpha\beta)^{-1} \\ 1 & 0 & 0 & (1+\alpha\beta)^{-1} \\ 0 & 1+(\alpha\beta)^{-1} & 0 & 0 \end{pmatrix} \in M_4(F).$$

Computations shows that $(\sigma(x)x + \beta^{-1}I_4)u \in \text{Alt}(M_4(F), t)$, where I_4 is the 4×4 identity matrix. By [5, (2.7)] we have $\sigma(x)x + \beta^{-1}I_4 \in \text{Alt}(M_4(F), \sigma)$, so $x \in S(M_4(F), \sigma)$. On the other hand

$$xu = \begin{pmatrix} 0 & \beta^{-1} & 1 & 0 \\ 0 & 0 & 0 & \alpha \\ 1 & 0 & 0 & 1 \\ 0 & \alpha + \beta^{-1} & 0 & 0 \end{pmatrix} \notin \text{Sym}(M_4(F), t),$$

which implies that $x \notin \text{Sym}(M_4(F), \sigma)$, thanks to [5, (2.7)]. It follows that $x \in S(M_4(F), \sigma) \setminus \text{Sym}(M_4(F), \sigma)$.

Lemma 3.13. *Let t be the transpose involution on $M_n(F)$. Then*

$$(i) \quad Q(q_t) = F^2.$$

$$(ii) \quad q_t \simeq \langle 1 \rangle_q \perp (n^2 - n) \times \langle 0 \rangle_q.$$

Proof. (i) Clearly, we have $F^2 \subseteq Q(q_t)$. The converse inclusion follows from Lemma 3.11 (ii) and the fact that the transpose involution is the adjoint involution of the bilinear form $n \times \langle 1 \rangle$ (see Proposition 2.1).

(ii) Using the first part and the isometry $\langle 1, 1 \rangle_q \simeq \langle 1, 0 \rangle_q$ we have $q_t \simeq \langle 1 \rangle_q \perp k \times \langle 0 \rangle_q$ for some non-negative integer k . We claim that $k = n^2 - n$. Let $W = \{x \in S(M_n(F), t) \mid q_t(x) = 0\}$. Then W is a k -dimensional vector space over F . A matrix $x = (x_{ij}) \in M_n(F)$ belongs to W if and only if $x^t x \in \text{Alt}(M_n(F), t)$. Note that $\text{Alt}(M_n(F), t)$ is the set of symmetric matrices with zero diagonal. Hence, $x^t x \in \text{Alt}(M_n(F), t)$ if and only if $\sum_{i=1}^n x_{ij}^2 = 0$ for $j = 1, \dots, n$, or equivalently

$$\sum_{i=1}^n x_{ij} = 0, \quad \text{for } j = 1, \dots, n. \quad (1)$$

Hence, W is the set of answers of the homogeneous system of linear equations (1) with n^2 unknowns x_{ij} , $i, j = 1, \dots, n$. This set is a vector space of dimension $n^2 - n$ over F , hence $k = n^2 - n$. \square

Theorem 3.14. *Let (A, σ) be a central simple algebra of degree n with orthogonal involution over F . If A splits, then $(A, \sigma) \simeq (M_n(F), t)$ if and only if $q_\sigma \simeq \langle 1 \rangle_q \perp (n^2 - n) \times \langle 0 \rangle_q$.*

Proof. The ‘only if’ implication follows from Lemma 3.5 and Lemma 3.13.

To prove the converse, we may identify $(A, \sigma) = (\text{End}_F(V), \sigma_{\mathfrak{b}})$, where (V, \mathfrak{b}) is a symmetric non-alternating bilinear space over F . By [6, (2.1)] there exist unique integers m, k and $a_1, \dots, a_m \in F$ such that

$$\mathfrak{b} \simeq \mathfrak{b}_{an} \perp \mathbb{M}(a_1) \perp \dots \perp \mathbb{M}(a_m) \perp k \times \mathbb{H}, \quad (2)$$

where \mathfrak{b}_{an} is an anisotropic bilinear form, $\mathbb{M}(a_i) = \langle a_i, a_i \rangle$ and \mathbb{H} is the hyperbolic plane. Let

$$U = \{x \in S(\text{End}_F(V), \sigma_{\mathfrak{b}}) \mid q_{\sigma_{\mathfrak{b}}}(x) = 0\} \quad \text{and} \quad W = \{v \in V \mid \mathfrak{b}(v, v) = 0\}.$$

Then U and W are two vector spaces over F . We have $\dim_F U = n^2 - n$, because $q_\sigma \simeq \langle 1 \rangle_q \perp (n^2 - n) \times \langle 0 \rangle_q$. Also, by [6, (2.1)] we have $\dim_F W = 2k + m$. On the other hand Lemma 3.11 (i) implies that $x(V) \subseteq W$ for every $x \in U$, i.e., $U \subseteq \text{Hom}_F(V, W)$. By dimension count we get $\dim_F W \geq n - 1$. However, we have $W \neq V$, because \mathfrak{b} is not alternating. Hence, $\dim_F W = n - 1$, i.e., $2k + m = n - 1$. By (2) we have $n = \dim_F \mathfrak{b}_{an} + 2k + 2m$, which implies that $\dim_F \mathfrak{b}_{an} + m = 1$. It follows that either \mathfrak{b}_{an} is trivial and $m = 1$ or $\dim_F \mathfrak{b}_{an} = 1$ and $m = 0$. Hence, either $\mathfrak{b} \simeq \langle \alpha, \alpha \rangle \perp k \times \mathbb{H}$ or $\mathfrak{b} \simeq \langle \alpha \rangle \perp k \times \mathbb{H}$ for some $\alpha \in F^\times$. Using the isometry $\langle \alpha \rangle \perp \mathbb{H} \simeq \langle \alpha, \alpha, \alpha \rangle$ in [4, (1.16)], we get $\mathfrak{b} \simeq n \times \langle \alpha \rangle$. Hence, $(A, \sigma) \simeq (M_n(F), t)$ by Proposition 2.1. \square

The next example shows that for $n > 2$ there exists a central simple algebra with orthogonal involution (A, σ) of degree n over F such that $q_\sigma = \langle 1 \rangle_q$. Note that for every algebra with involution (A, σ) over F we have $F \subseteq S(A, \sigma)$. Hence, the form $\langle 1 \rangle_q$ is always a subform of the alternator form q_σ .

Example 3.15. For $\alpha_1, \dots, \alpha_n \in F^\times$ let u be the diagonal $n \times n$ matrix $\text{diag}(\alpha_1, \dots, \alpha_n)$ and consider the involution $\sigma = \text{Int}(u) \circ t$ on $M_n(F)$. Let $\mathfrak{b} = \langle \alpha_1, \dots, \alpha_n \rangle$. By Proposition 2.1 we have $(M_n(F), \sigma) \simeq (\text{End}_F(V), \sigma_{\mathfrak{b}})$, where V is an underlying vector space of \mathfrak{b} . Let $x = (x_{ij}) \in M_n(F)$. We first claim that $x \in S(M_n(F), \sigma)$ with $q_\sigma(x) = \lambda \in F$ if and only if

$$\alpha_1^{-1} x_{1i}^2 + \dots + \alpha_n^{-1} x_{ni}^2 = \alpha_i^{-1} \lambda \quad \text{for } i = 1, \dots, n. \quad (3)$$

By definition $x \in S(M_n(F), \sigma)$ (with $q_\sigma(x) = \lambda$) if and only if

$$y := \sigma(x)x + \lambda I_n \in \text{Alt}(M_n(F), \sigma).$$

By [5, (2.4)] we have $\text{Alt}(M_n(F), \sigma) = u \cdot \text{Alt}(M_n(F), t)$, so $y \in \text{Alt}(M_n(F), \sigma)$ if and only if $u^{-1}y \in \text{Alt}(M_n(F), t)$. Since $y \in \text{Sym}(M_n(F), \sigma)$ we have $u^{-1}y \in \text{Sym}(M_n(F), t)$ by [5, (2.4)]. Hence, $x \in S(M_n(F), \sigma)$ if and only if $u^{-1}y$ has zero diagonal. Write $u^{-1}y = (y_{ij})$ for some $y_{ij} \in F$, $1 \leq i, j \leq n$. As $y = ux^t u^{-1}x + \lambda I_n$, computation shows that

$$y_{ii} = \alpha_1^{-1} x_{1i}^2 + \dots + \alpha_n^{-1} x_{ni}^2 + \alpha_i^{-1} \lambda \quad \text{for } i = 1, \dots, n.$$

We have $y_{ii} = 0$ if and only if (3) is satisfied, as claimed.

Now, if $n > 2$ and $\langle \alpha_1, \dots, \alpha_n \rangle$ is an anisotropic bilinear Pfister form, then (3) implies that $\lambda = x_{11}^2 = \dots = x_{nn}^2$ and $x_{ij} = 0$ for $i \neq j$. It follows that $\lambda \in F^2$ and x is a scalar (matrix). Hence, $S(A, \sigma) = F$ and $q_\sigma = \langle 1 \rangle_q$.

Remark 3.16. Example 3.15 shows that the alternator form does not necessarily classify orthogonal involutions on a given central simple algebra. Also, using Example 3.15 one can show that the inclusion $Q(q_{\sigma_{\mathfrak{b}}}) \subseteq Q(\mathfrak{b})$ in Lemma 3.11 could be strict. Indeed, with the notation of Example 3.15 set $\mathfrak{b}' = \alpha_1 \cdot \mathfrak{b}$. Then \mathfrak{b}' represents 1 and $(\text{End}_F(V), \sigma_{\mathfrak{b}}) \simeq (\text{End}_F(V), \sigma_{\mathfrak{b}'})$ (see [5, p. 1]). By Lemma 3.5 we have $Q(q_{\sigma_{\mathfrak{b}'}}) = Q(q_{\sigma_{\mathfrak{b}}}) = F^2$. Since \mathfrak{b} is anisotropic we have $\alpha_2 \notin F^2$, hence $\alpha_2 \in Q(\mathfrak{b}') \setminus Q(q_{\sigma_{\mathfrak{b}'}})$.

4 Applications to totally decomposable involutions

A *quaternion algebra* over F is a central simple algebra of degree 2. An algebra with involution (A, σ) over F is called *totally decomposable* if it decomposes

into tensor products of quaternion F -algebras with involution. Let $(A, \sigma) \simeq \bigotimes_{i=1}^n (Q_i, \sigma_i)$ be a totally decomposable algebra with orthogonal involution over F . By [5, (2.23)] every σ_i is an orthogonal involution. Write $\text{disc } \sigma_i = \alpha_i F^{\times 2} \in F^{\times} / F^{\times 2}$ for some $\alpha_i \in F^{\times}$, $i = 1, \dots, n$. As in [3] we denote the bilinear Pfister form $\langle\langle \alpha_1, \dots, \alpha_n \rangle\rangle$ by $\mathfrak{Pf}(A, \sigma)$. By [3, (7.5)], $\mathfrak{Pf}(A, \sigma)$ is independent of the decomposition of (A, σ) . Also, as observed in [7] there exists a unique, up to isomorphism, F -algebra $\Phi(A, \sigma) \subseteq F \oplus \text{Alt}(A, \sigma)$ of dimension 2^n satisfying: (i) $x^2 \in F$ for $x \in \Phi(A, \sigma)$; (ii) the centralizer of $\Phi(A, \sigma)$ in A coincides with $\Phi(A, \sigma)$ itself; (iii) $\Phi(A, \sigma)$ is generated, as an F -algebra by n elements. According to [7, (5.5)] the algebra $\Phi(A, \sigma)$ may be considered as an underlying vector space of $\mathfrak{Pf}(A, \sigma)$ such that

$$\mathfrak{Pf}(A, \sigma)(x, x) = x^2 \quad \text{for } x \in \Phi(A, \sigma).$$

Finally, let $x \in \Phi(A, \sigma)$ and set $\alpha = x^2 \in F$. Then $\sigma(x)x + \alpha = x^2 + \alpha = 0 \in \text{Alt}(A, \sigma)$. Hence, $\Phi(A, \sigma) \subseteq S(A, \sigma)$ and

$$q_{\sigma}(x) = \mathfrak{Pf}(A, \sigma)(x, x) = x^2 \quad \text{for } x \in \Phi(A, \sigma).$$

The following theorem complements some results in [3] and [7].

Theorem 4.1. *For a totally decomposable algebra with orthogonal involution (A, σ) over F the following conditions are equivalent: (1) σ is anisotropic. (2) σ is direct. (3) $\mathfrak{Pf}(A, \sigma)$ is anisotropic. (4) q_{σ} is anisotropic. (5) $\Phi(A, \sigma)$ is a field. (6) $S(A, \sigma)$ is a field. (7) $\Phi(A, \sigma) = S(A, \sigma)$. (8) $S(A, \sigma) \subseteq \text{Sym}(A, \sigma)$. In particular, if these conditions hold, the algebra $\Phi(A, \sigma)$ is uniquely determined.*

Proof. The equivalences (1) \Leftrightarrow (2) \Leftrightarrow (3) can be found in [3] (see [3, (6.1), (6.2) and (7.5)]). The equivalences (2) \Leftrightarrow (4) \Leftrightarrow (6) are proved in Theorem 3.7 and (1) \Leftrightarrow (5) follows from [7, (6.6)] and [3, (6.2)]. Suppose that $S(A, \sigma)$ is a field. Since $\Phi(A, \sigma) \subseteq S(A, \sigma)$ and $\Phi(A, \sigma)$ is maximal commutative, we get $\Phi(A, \sigma) = S(A, \sigma)$. This proves (6) \Rightarrow (7). The implication (7) \Rightarrow (8) is evident and (8) \Rightarrow (2) follows from Proposition 3.9. \square

Lemma 4.2. *Let K/F be a separable quadratic extension and let \mathfrak{b} be a symmetric bilinear form over F . Then $D(\mathfrak{b}_K) \cap F = D(\mathfrak{b})$.*

Proof. Clearly, we have $D(\mathfrak{b}) \subseteq D(\mathfrak{b}_K) \cap F$. Suppose that $\alpha \in D(\mathfrak{b}_K) \cap F$. Let V be an underlying vector space of \mathfrak{b} . Write $K = F(\eta)$ for some $\eta \in K$ with $\delta := \eta^2 + \eta \in F$. Then $\alpha = \mathfrak{b}_K(u \otimes 1 + v \otimes \eta, u \otimes 1 + v \otimes \eta)$ for some $u, v \in V$. Thus

$$\begin{aligned} \alpha &= (\mathfrak{b}(u, u) + \delta \mathfrak{b}(v, v)) + \eta(\mathfrak{b}(u, v) + \mathfrak{b}(v, u) + \mathfrak{b}(v, v)) \\ &= (\mathfrak{b}(u, u) + \delta \mathfrak{b}(v, v)) + \eta \mathfrak{b}(v, v). \end{aligned}$$

Since $\alpha \in F$ we get $\mathfrak{b}(v, v) = 0$. Hence, $\alpha = \mathfrak{b}(u, u) \in D(\mathfrak{b})$, proving the result. \square

Proposition 4.3. *If (A, σ) is a totally decomposable algebra with orthogonal involution over F , then $D(q_{\sigma}) = D(\mathfrak{Pf}(A, \sigma))$.*

Proof. Let $\mathfrak{b} = \mathfrak{Pf}(A, \sigma)$. Since $\mathfrak{b}(x, x) = x^2 = q_\sigma(x)$ for every $x \in \Phi(A, \sigma) \subseteq S(A, \sigma)$ we have $D(\mathfrak{b}) \subseteq D(q_\sigma)$. To prove the converse inclusion, let $(A, \sigma) \simeq \bigotimes_{i=1}^n (Q_i, \sigma_i)$ be a decomposition of (A, σ) into quaternion algebras with involution. For $i = 0, \dots, n$, define a field K_i inductively as follows: set $K_0 = F$ and suppose that K_i is defined. If K_i splits A , set $K_{i+1} = K_i$. Otherwise, let r be the minimal number for which K_i does not split Q_r . Then $Q_r \otimes_F K_i$ is a division algebra over K_i . Let K_{i+1} be a maximal separable subfield of $Q_r \otimes K_i$. Note that for $i = 0, \dots, n-1$, K_i may be identified with a subfield of K_{i+1} . Also, either $K_{i+1} = K_i$ or K_{i+1}/K_i is a separable quadratic extension. Set $L := K_n$, so that A_L splits.

By [3, (7.5)], we may identify $(A, \sigma)_L = (\text{End}_L(V), \sigma_{\mathfrak{b}_L})$. Using Lemma 3.11 we get $D(q_{\sigma_L}) \subseteq D(\mathfrak{b}_L)$. If $x \in S(A, \sigma)$ and $\alpha = q_\sigma(x)$, then $x \otimes 1 \in S((A, \sigma)_L)$ and $q_{\sigma_L}(x \otimes 1) = \alpha \otimes 1$. Hence, by identifying $F \otimes F \subseteq A \otimes F$ with F we have $D(q_\sigma) \subseteq D(q_{\sigma_L})$. It follows that $D(q_\sigma) \subseteq D(\mathfrak{b}_L)$. By 4.2 and induction on n we have $D(\mathfrak{b}_L) \cap F = D(\mathfrak{b}) \subseteq D(q_\sigma)$. Hence, $D(q_\sigma) \subseteq D(\mathfrak{b})$, proving the result. \square

Lemma 4.4. *Let \mathfrak{b} and \mathfrak{b}' be two isotropic bilinear n -fold Pfister forms over F . Then $\mathfrak{b} \simeq \mathfrak{b}'$ if and only if $Q(\mathfrak{b}) = Q(\mathfrak{b}')$.*

Proof. The ‘only if’ implication is evident. To prove the converse, choose positive integers r and r' and anisotropic bilinear Pfister forms \mathfrak{c} and \mathfrak{c}' over F such that $\mathfrak{b} \simeq \langle\langle 1 \rangle\rangle^r \otimes \mathfrak{c}$ and $\mathfrak{b}' \simeq \langle\langle 1 \rangle\rangle^{r'} \otimes \mathfrak{c}'$, where $\langle\langle 1 \rangle\rangle^s$ is the s -fold Pfister form $\langle\langle 1, \dots, 1 \rangle\rangle$ (see [1, p. 909]). Since \mathfrak{c} and \mathfrak{c}' are anisotropic we have $\dim_{F^2} Q(\mathfrak{c}) = 2^{n-r}$ and $\dim_{F^2} Q(\mathfrak{c}') = 2^{n-r'}$. As $Q(\mathfrak{b}) = Q(\mathfrak{c})$ and $Q(\mathfrak{b}') = Q(\mathfrak{c}')$, the assumption implies that $Q(\mathfrak{c}) = Q(\mathfrak{c}')$, hence $r = r'$. The conclusion now follows from [1, (A.8)]. \square

Corollary 4.5. *Let (A, σ) and (A', σ') be totally decomposable algebras with isotropic orthogonal involution over F . If $q_\sigma \simeq q_{\sigma'}$ then $\mathfrak{Pf}(A, \sigma) \simeq \mathfrak{Pf}(A', \sigma')$.*

Proof. The result follows from Proposition 4.3 and Lemma 4.4. \square

Theorem 4.6. *Let (A, σ) and (A', σ') be totally decomposable algebras with isotropic orthogonal involution over F . Then $(A, \sigma) \simeq (A', \sigma')$ if and only if $A \simeq A'$ and $q_\sigma \simeq q_{\sigma'}$.*

Proof. The ‘only if’ implication follows from Lemma 3.5 and the converse follows from Corollary 4.5 and [7, (6.5)]. \square

Notation 4.7. Let (A, σ) be a totally decomposable algebra with anisotropic orthogonal involution over F . By Theorem 4.1 we have $S(A, \sigma) = \Phi(A, \sigma) \subseteq F \oplus \text{Alt}(A, \sigma)$. We denote the set $S(A, \sigma) \cap \text{Alt}(A, \sigma)$ by $S'(A, \sigma)$. We also denote by q'_σ the restriction of q_σ to $S'(A, \sigma)$.

Note that we have $S(A, \sigma) = F \oplus S'(A, \sigma)$ and $q_\sigma \simeq \langle 1 \rangle_q \perp q'_\sigma$, because $q_\sigma(1) = 1$. Also, as observed in [7, p. 223] one has an orthogonal decomposition $\Phi(A, \sigma) = F \perp S'(A, \sigma)$ with respect to $\mathfrak{Pf}(A, \sigma)$. It follows that $q'_\sigma(x) = x^2 = \mathfrak{b}'(x, x)$ for $x \in S'(A, \sigma)$, where \mathfrak{b}' is the pure subform of $\mathfrak{Pf}(A, \sigma)$. Hence, we have the following result (recall that for a symmetric bilinear space (V, \mathfrak{b}) over F , there exists a unique totally singular quadratic form $\varphi_{\mathfrak{b}}$ on V given by $\varphi_{\mathfrak{b}}(x) = \mathfrak{b}(x, x)$).

Lemma 4.8. *Let (A, σ) be a totally decomposable algebra with anisotropic orthogonal involution over F and let $\mathfrak{b} = \mathfrak{Pf}(A, \sigma)$. Then $q_\sigma = \varphi_{\mathfrak{b}}$ and $q'_\sigma = \varphi_{\mathfrak{b}'}$, where \mathfrak{b}' is the pure subform of \mathfrak{b} .*

Let (A, σ) be a totally decomposable algebra of degree 2^n with orthogonal involution over F . Then there exists a set $\{v_1, \dots, v_n\}$ consisting of units such that $\Phi(A, \sigma) \simeq F[v_1, \dots, v_n]$ and $v_{i_1} \cdots v_{i_s} \in \text{Alt}(A, \sigma)$ for every $1 \leq s \leq n$ and $1 \leq i_1 < \dots < i_s \leq n$ (see [7, (5.1)] for more details). As in [7] we call $\{v_1, \dots, v_n\}$ a *set of alternating generators* of $\Phi(A, \sigma)$. According to [7, (5.3) and (5.5)], if $\{v_1, \dots, v_n\}$ is a set of alternating generators of $\Phi(A, \sigma)$ and $\alpha_i = v_i^2 \in F^\times$ for $i = 1, \dots, n$, then $\mathfrak{Pf}(A, \sigma) \simeq \langle\langle \alpha_1, \dots, \alpha_n \rangle\rangle$.

Proposition 4.9. *Let (A, σ) and (A', σ') be totally decomposable algebras with anisotropic orthogonal involution over F . Then $q'_\sigma \simeq q'_{\sigma'}$ if and only if $\mathfrak{Pf}(A, \sigma) \simeq \mathfrak{Pf}(A', \sigma')$.*

Proof. The ‘if’ implication follows from Lemma 4.8. To prove the converse, let $\deg_F A = 2^n$ and let $\{x_1, \dots, x_n\}$ be a set of alternating generators of $\Phi(A, \sigma)$. Set $\alpha_i = x_i^2 \in F^\times$, so that $\mathfrak{Pf}(A, \sigma) \simeq \langle\langle \alpha_1, \dots, \alpha_n \rangle\rangle$. By dimension count the set

$$\{x_{i_1} \cdots x_{i_s} \mid 1 \leq s \leq n \text{ and } 1 \leq i_1 < \dots < i_s \leq n\},$$

is a basis of $S'(A, \sigma)$ over F . Let $f : (S'(A, \sigma), q'_\sigma) \xrightarrow{\sim} (S'(A', \sigma'), q'_{\sigma'})$ be an isometry and set $x'_i = f(x_i) \in S'(A', \sigma')$, $i = 1, \dots, n$. Then

$$x_i'^2 = q'_{\sigma'}(x'_i) = q'_\sigma(x_i) = \alpha_i \quad \text{for } i = 1, \dots, n. \quad (4)$$

We claim that $f(x_{i_1} \cdots x_{i_s}) = x'_{i_1} \cdots x'_{i_s}$ for $1 \leq s \leq n$ and $1 \leq i_1 < \dots < i_s \leq n$. Since $S(A', \sigma')$ is an F -algebra we have $x'_{i_1} \cdots x'_{i_s} \in S(A', \sigma')$. We also have

$$\begin{aligned} q_{\sigma'}(f(x_{i_1} \cdots x_{i_s}) + x'_{i_1} \cdots x'_{i_s}) &= q_\sigma(x_{i_1} \cdots x_{i_s}) + q_{\sigma'}(x'_{i_1} \cdots x'_{i_s}) \\ &= (x_{i_1} \cdots x_{i_s})^2 + (x'_{i_1} \cdots x'_{i_s})^2. \end{aligned} \quad (5)$$

Since $S(A, \sigma) = \Phi(A, \sigma)$, $S(A, \sigma)$ is commutative. Similarly, $S(A', \sigma')$ is also commutative. Hence, using (5) and (4) we get

$$q_{\sigma'}(f(x_{i_1} \cdots x_{i_s}) + x'_{i_1} \cdots x'_{i_s}) = x_{i_1}^2 \cdots x_{i_s}^2 + x_{i_1}'^2 \cdots x_{i_s}'^2 = 0.$$

As $q_{\sigma'}$ is anisotropic we get $f(x_{i_1} \cdots x_{i_s}) = x'_{i_1} \cdots x'_{i_s}$, proving the claim. In particular, we have $x'_{i_1} \cdots x'_{i_s} \in S'(A', \sigma') \subseteq \text{Alt}(A', \sigma')$ for $1 \leq s \leq n$ and $1 \leq i_1 < \dots < i_s \leq n$. Hence, $\{x'_1, \dots, x'_n\}$ is a set of alternating generators of $\Phi(A', \sigma')$. The relation (4) now implies that $\mathfrak{Pf}(A', \sigma') \simeq \langle\langle \alpha_1, \dots, \alpha_n \rangle\rangle \simeq \mathfrak{Pf}(A, \sigma)$. \square

Using Lemma 3.5, [7, (6.5)] and Proposition 4.9 we have the following analogue of Theorem 4.6.

Theorem 4.10. *Let (A, σ) and (A', σ') be totally decomposable algebras with anisotropic orthogonal involution over F . Then $(A, \sigma) \simeq (A', \sigma')$ if and only if $A \simeq A'$ and $q'_\sigma \simeq q'_{\sigma'}$.*

References

- [1] J. Arason, R. Baeza, Relations in I^n and $I^n W_q$ in characteristic 2. *J. Algebra* **314** (2007), no. 2, 895–911.
- [2] A. Dolphin, Decomposition of algebras with involution in characteristic 2. *J. Pure Appl. Algebra* **217** (2013), no. 9, 1620–1633.
- [3] A. Dolphin, Orthogonal Pfister involutions in characteristic two. *J. Pure Appl. Algebra* **218** (2014), no. 10, 1900–1915.
- [4] R. Elman, N. Karpenko, A. Merkurjev, *The algebraic and geometric theory of quadratic forms*. American Mathematical Society Colloquium Publications, 56. American Mathematical Society, Providence, RI, 2008.
- [5] M.-A. Knus, A. S. Merkurjev, M. Rost, J.-P. Tignol, *The book of involutions*. American Mathematical Society Colloquium Publications, 44. American Mathematical Society, Providence, RI, 1998.
- [6] A. Laghribi, P. Mammone. Hyper-isotropy of bilinear forms in characteristic 2. *Contemporary Mathematics*, **493** (2009), 249-269.
- [7] M. G. Mahmoudi, A.-H. Nokhodkar, On totally decomposable algebras with involution in characteristic two. *J. Algebra* **451** (2016), 208–231.

A.-H. NOKHODKAR, anokhodkar@yahoo.com,
DEPARTMENT OF PURE MATHEMATICS, FACULTY OF SCIENCE, UNIVERSITY OF KASHAN, P. O.
BOX 87317-51167, KASHAN, IRAN.